UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/321,839	05/28/99	PENSAK	D 11953.0002

TM02/0111

STEPTOE & JOHNSON LLP
1330 CONNECTICUT AVENUE NW
WASHINGTON DC 20036-1795

EXAMINER	
SULTZIN, B.	
ART UNIT	**PAPER NUMBER**
2132	7

DATE MAILED: 01/11/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 09/321,839	Applicant(s) PENSAK ET AL.	
	Examiner Ronald F. Sulpizio	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 October 2000* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

15) ☐ Notice of References Cited (PTO-892)
16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
18) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other: .

DETAILED ACTION

Response to Amendment and Arguments

1. The amendment filed 18 October 2000 has been considered but is ineffective to overcome the 35 USC § 103 rejection.

2. Applicant's arguments with respect to Claims 1-3 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments are based on amendments made to Claims 1 and 3.

3. The amendment filed on 16 October 2000 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

- Claims 1, 4, and 10 – the "in response to" language is not in the specification. The language implies no intervening steps, however, the specification describes no such relationship between steps as on p. 4 of the specification where it says, "[t]he viewing tool . . . decrypts the document into clear text, renders the document segment, and destroys the decryption key and the clear text version of the document segment". And on p. 14 the specification says, "The Plug-In at the authoring user's computer encrypts the segment, immediately destroys or removes the key from the authoring user's machine, and then deletes the clear text for the segment from the Plug-In."

Allowable Subject Matter

4. Claims 10-14 are rejected as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and the 35 USC § 112 rejection is overcome.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1, 4, and 10 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- Claims 1, 4, and 10 – the "in response to" language" is not in the specification. The language implies no intervening steps, however, the specification describes no such relationship between steps as on p. 4 of the specification where it says, "[t]he viewing tool . . . decrypts the document into clear text, renders the document segment, and destroys the decryption key and the clear text version of the document segment". And on p. 14 the specification says, "The Plug-In at the authoring user's computer encrypts the segment, immediately destroys or removes the key from the authoring user's machine, and then deletes the clear text for the segment from the Plug-In."

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson (US Patent 5,765,152) and Saito (US Patent 6,002,772) or Akiyama et al. (US Patent 5,440,631).

Claims 1

Erickson teaches a method of controlling distribution of electronic information comprising the steps of:

- retrieving, at a user location, a segment of encrypted electronic information (Erickson Col. 19, Lines 1-5, Col. 26, Lines 5-10);
- receiving, from a key server, a copy of a decryption key for the segment (Erickson Col. 16, Lines 55-64), and at least one user limitation assigned to the segment and associated with the decryption key (Erickson Col. 16, Lines 60-64);
- accessing the segment using the copy of the decryption key at the user location for the segment and a control process the control process responsive to a user limitation to control distribution of the electronic information (Erickson Col. 16, Lines 55-64; Col. 20, Lines 17-21; Col. 22, Lines 48-65);
- displaying a decrypted segment in response to an accessing (Erickson Col. 25, Lines 47-54)

Erickson, however, fails to teach destroying the copy of the **decryption key** at the user location in response to accessing the segment. Saito and Akiyama et al., on the other hand, teach this (See Saito Col. 16, Lines 1-10 and Figure 4A and Akiyama et al. Col. 17 Lines 45-60 where the number of N repetitions equals 1). In light of Saito or Akiyama et al, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify Erickson's system to include the destruction of the decryption key, than not modify it, in order to hinder subsequent unauthorized use of the decryption key and access to the electronic information.

Erickson, additionally fails to specifically to teach destroying a **decrypted segment** in response to displaying. Akiyama et al., on the other hand, teaches this (See Akiyama et al. Col. 17, Lines 60-69 and Col. 18, Lines 28-35 where destruction of the segment is inherent). In light of Akiyama et al., it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Erickson to include destroying a decrypted segment in response to displaying, than not modify it, in order to prevent the undue profit which a person who illegally uses information stored in a piece of storage medium may obtain. (See Akiyama et al. Col. 18, Lines 28-35).

Claim 2

Erickson teaches the method of controlling distribution of electronic information as in claim 1 above, wherein access to the decryption key is controlled by the key server subject to unique segment identification associated with the segment and the user limitation associated with the segment (Erickson Col. 18, Lines 3-10).

Claims 3

Erickson teaches a method of controlling distribution of electronic information comprising the steps of:

- retrieving, at a user location, a first encrypted segment of encrypted electronic information (Erickson Col. 19, Lines 1-5, Col. 26, Lines 5-10);
- receiving, from a key server, a copy of a first decryption key for the first segment (Erickson Col. 16, Lines 55-64), and at least one user limitation assigned to the first segment and associated with the first decryption key (Erickson Col. 16, Lines 60-64);
- accessing the first segment using the copy of the decryption key at the user location for the first segment. (Erickson Col. 16, Lines 55-64; Col. 20, Lines 17-21; Col. 22, Lines 48-65);

Erickson, however, fails to teach destroying the copy of the **decryption key** for a first segment. Saito and Akiyama et al., on the other hand, teach this (See Saito Col. 16, Lines 1-10 and Figure 4A and Akiyama et al. Col. 17 Lines 45-60 where the number of N repetitions equals 1). In light of Saito or Akiyama et al, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify Erickson's system to include the destruction of the decryption key, than not modify it, in order to prevent subsequent unauthorized use of the decryption key and access to the electronic information.

Erickson also fails to teach receiving a decryption key for accessing a second segment of the electronic document after destroying the first decryption key. Official notice is taken that it is old and well known in the cryptographic arts to receive a decryption key for accessing a second segment of an electronic document after destroying the first key (particularly in an asynchronous system, or where a key was previously lost, or where a computer is turned off and then on again

between the viewing of encrypted document segments) to get the advantage of accessing a second segment, preventing subsequent and immediate unauthorized use of the first decryption key. It would have been obvious to one of ordinary skilled in the art at the time of the Applicant's invention to modify the system of Erickson, then not modify it, to get this advantage.

Claim 4

Erickson teaches viewing encrypted electronic information on a display, comprising:

- retrieving, at a user location, a segment of encrypted electronic information; (Erickson Col. 19, Lines 1-5, Col. 26, Lines 5-10);
- receiving, from a remote server, a decryption key for the segment; (Erickson Col. 16, Lines 55-64),
- decrypting the segment using the decryption key; (Erickson Col. 16, Lines 55-64; Col. 20, Lines 17-21; Col. 22, Lines 48-65);
- displaying the segment as decrypted on the display; (Erickson Col. 25, Lines 47-54)

Erickson, however, fails to teach destroying the copy of the **decryption key** at the user location in response to decrypting the segment. Saito and Akiyama et al., on the other hand, teach this (See Saito Col. 16, Lines 1-10 and Figure 4A and Akiyama et al. Col. 17 Lines 45-60 where the number of N repetitions equals 1). In light of Saito or Akiyama et al, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify Erickson's system to include the destruction of the decryption key, than not modify it, in order to prevent subsequent unauthorized use of the decryption key and access to the electronic information.

Erickson, additionally fails to specifically to teach destroying a **decrypted segment** in

response to displaying. Akiyama et al., on the other hand, teaches this (See Akiyama et al. Col. 17, Lines 60-69 and Col. 18, Lines 28-35 where destruction of the segment is inherent). In light of Akiyama et al., it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Erickson to include destroying a decrypted segment in response to displaying, than not modify it, in order to prevent the undue profit which a person who illegally uses information stored in a piece of storage medium may obtain. (See Akiyama et al. Col. 18, Lines 28-35).

Claim 5

Erickson teaches an encrypted communication channel, wherein the receiving of decryption key occurs (Erickson Col. 16, Lines 55-60). Additionally, Official notice is taken that it is old and well known in the cryptographic arts to encrypt the channel a decryption key is received on to get the advantage of a key safe from compromise. It would have been obvious to one of ordinary skilled in the art at the time of the Applicant's invention to modify the system of Erickson (if Erickson did not include this), then not modify it, to get this advantage.

Claim 6

Erickson teaches entering user identification information, receiving the decryption key being responsive to said user identification information representing at least one of an authorized user and authorized conditions (Erickson Col. 20, Lines 50-67; Col. 16, Lines 55-64). Additionally, official notice is taken that it is old and well known in the cryptographic arts to gain access to a decryption key after showing that one is an authorized user under authorized conditions (e.g. this also typically occurs when a company's CA gives a key to an employee) to get the advantage of limited key distribution and document privacy. It would

have been obvious to one of ordinary skilled in the art at the time of the Applicant's invention to modify the system of Erickson (if Erickson did not include this), then not modify it, to get this advantage.

Claim 7

Erickson teaches limiting access to the segment at the user location consistent with predetermined criteria associated with at least one of the segment and user identification information. (Erickson Col. 16, Lines 43-64)

Claim 8

Erickson teaches changing the predetermined criteria associated with the segment and user identification information. (Erickson Col. 16, Lines 43-64; Col 20, Lines 50-67; Col. 22, Lines 48-65)

Claim 9

Erickson fails to teach destroying, at a remote server, a decryption key. Official notice is taken that it is old and well known in the cryptographic arts to destroy a decryption key where it is stored and distributed to get the advantage of hindering the further propagation of decrypted information of which the key was meant to decrypt. It would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Erickson, then not modify it, to get this advantage.

Claim 19

Erickson teaches accessing encrypted information, comprising:

- retrieving a first encrypted information (Erickson Col. 19, Lines 1-5, Col. 26, Lines 5-10);
- receiving, from a remote server, a first decryption key;

  (Erickson Col. 16, Lines 60-64);
- accessing the first encrypted information with the first decryption key;

  (Erickson Col. 16, Lines 55-64; Col. 20, Lines 17-21; Col. 22, Lines 48-65);

Erickson, however, fails to teach destroying, at the user location, the decryption key for a first segment. Saito and Akiyama et al., on the other hand, teach this (See Saito Col. 16, Lines 1-10 and Figure 4A and Akiyama et al. Col. 17 Lines 45-60 where the number of N repetitions equals 1). In light of Saito or Akiyama et al, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify Erickson's system to include the destruction of the decryption key, than not modify it, in order to prevent subsequent unauthorized use of the decryption key and access to the electronic information.

Erickson also fails to teach receiving a decryption key for accessing a second segment of the electronic document after destroying the first decryption key. Official notice is taken that it is old and well known in the cryptographic arts to receive a decryption key for accessing a second segment of an electronic document after destroying the first key (particularly in an asynchronous system, or where a key was previously lost, or where a computer is turned off and then on again between the viewing of encrypted document segments) to get the advantage of accessing a second segment, preventing subsequent and immediate unauthorized use of the first decryption key. It would have been obvious to one of ordinary skilled in the art at the time of the Applicant's invention to modify the system

of Erickson, then not modify it, to get this advantage.

9. Claims 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Erickson (US Patent 5,765,152).

Claim 15

Erickson teaches:

- first, sending the first decryption key to a user location; (Erickson Col. 16, Lines 55-64),

Erickson, however, fails to teach generating, at a server, first and second encryption keys and associated first and second decryption keys, respectively. Official notice is taken that it is old and well known in the cryptographic arts to generate first and second encryption and decryption keys at a server (particularly in a large enterprise) to get the advantages of providing new keys to individuals in the event their keys are lost or destroyed, while at the same time maintaining the ability to decrypt documents using keys that were lost or destroyed by users. It would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Erickson, then not modify it, to get this advantage.

Erickson, additionally, fails to teach sending a second decryption key to a user location after destruction, to the user location, of the first decryption key. Official notice is taken that it is old and well known in the cryptographic arts to provide a user a second key after the first one has been destroyed to get the advantage of a user that can continue decrypting information sent to him using a new key pair. It would have been obvious to one of ordinary skill in the art at the

time of the Applicant's invention to modify the system of Erickson, then not modify it, to get this advantage.

Claim 16

Erickson teaches entering user identification information, receiving the decryption key being responsive to said user identification information representing at least one of an authorized user and authorized conditions (Erickson Col. 20, Lines 50-67; Col. 16, Lines 55-64). Additionally, official notice is taken that it is old and well known in the cryptographic arts to gain access to a decryption key after showing that one is an authorized user under authorized conditions (e.g. this also typically occurs when a company's CA gives a key to an employee) to get the advantage of limited key distribution and document privacy. It would have been obvious to one of ordinary skilled in the art at the time of the Applicant's invention to modify the system of Erickson (if Erickson did not include this), then not modify it, to get this advantage.

Claim 17

Erickson fails to specifically teach recording each instance of a first and second sending of decryption keys. Official notice is taken that it is old and well known in the cryptographic arts to record the sending of keys to get the advantage of knowing who got what keys and knowing which decryption key to recover in the event one gets lost or destroyed. It would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Erickson, then not modify it, to get this advantage.

Claim 18

Erickson does not specifically teach destroying, at the server, the first and second decryption keys. Official notice is taken that it is old and well known in the cryptographic arts to destroying of a first and second decryption key to get the advantage of hindering subsequent unauthorized use of the decryption key and access to the electronic information. It would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Erickson, then not modify it, to get this advantage.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ronald F. Sulpizio whose telephone number is (703) 308-2391.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod R. Swann can be reached on (703) 308-7791. The fax phone numbers for the

organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-5065 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9700.

Ronald F. Sulpizio
Examiner
Art Unit 2132

RFS
9 January, 2001

TOD SWANN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100